UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/057,043 | 01/25/2002 | Ranga S. Ramanujan | 1032-001US01 | 3446 |

28863 7590 06/13/2007

SHUMAKER & SIEFFERT, P. A.
1625 RADIO DRIVE
SUITE 300
WOODBURY, MN 55125

| EXAMINER | |
|---|---|
| GILLIS, BRIAN J | |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2141 | |

| MAIL DATE | DELIVERY MODE |
|---|---|
| 06/13/2007 | PAPER |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 10/057,043 | RAMANUJAN ET AL. | |
| | Examiner | Art Unit | |
| | Brian J. Gillis | 2141 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *30 April 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-4,6,7,9-17,27,29,30,35-39,41,42,44-46,53 and 55* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-4,6,7,9-17,27,29,30,35-39,41,42,44-46,53 and 55* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *25 January 2002* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

## DETAILED ACTION

### *Claim Rejections - 35 USC § 103*

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

Claims 1, 3, 4, 6, 7, 9-11, 13, 14, 27, 30, 35, 37-39, 41-44, 53, and 55 are rejected under 35 U.S.C. 103(a) as being unpatentable over Genty et al (US Patent #6,473,863) in view of Afek et al (US PGPUB US2002/0083175) in view of Maeshima et al (US Patent #6,092,113).

Claim 1 discloses a method comprising: establishing a packet tunnel between a first local area network and a second local area network, the packet tunnel having a source network address within an address space of the first local area network and a destination network address within an address space of the second local area network;

reserving for the packet tunnel an amount of bandwidth within an access link; detecting a network attack; in response to the detected network attack, splitting the packet tunnel by selecting an intermediate network device, wherein the intermediate network device has a network address from a network address space other than the address space of the first local area network and the address space of the second local area network; establishing a first packet tunnel from the first local area network to the intermediate network device; establishing a second packet tunnel that originates from the intermediate network device to the second local area network; canceling the reserved bandwidth for the packet tunnel; reserving fro the second packet tunnel an amount of bandwidth within the access link; and communicating a virtual private network (VPN) traffic from the first local area network to the second local area network by redirecting the VPN traffic from the first local area network to the intermediate network device through the first packet tunnel and forwarding the VPN traffic from the intermediate network device to the second local area network through the second packet tunnel. Genty et al teaches a tunnel between a source and destination (figure 7), an attack is detected (column 5, lines 48-52), a secondary tunnel can be established with different addresses (column 5, lines 63-67 – column 6, lines 1-6, 20-24), a secondary tunnel is established (figure 7), and upon detecting a network attack canceling the bandwidth in the packet tunnel (column 6, lines 31-33). It fails to teach of reserving for the packet tunnels an amount of bandwidth within an access link, in response to the detected network attack, splitting the packet tunnel by selecting an intermediate network device, wherein the intermediate network device has a network address from a network address

space other than the address space of the first local area network and the address space of the second local area network, establishing a first packet tunnel from the first local area network to the intermediate network device, establishing a second packet tunnel that originates from the intermediate network device to the second local area network, canceling the reserved bandwidth for the packet tunnel and communicating a virtual private network (VPN) traffic from the first local area network to the second local area network by redirecting the VPN traffic from the first local area network to the intermediate network device through the first packet tunnel and forwarding the VPN traffic from the intermediate network device to the second local area network through the second packet tunnel. Afek et al teaches a different networks are connected together (paragraph 245), data is diverted to the guards upon detection of an attack which can be from another LAN (paragraphs 250, 252, and 253), data is directed from the source to the guard (paragraph 267), data is sent from the guard to the target (paragraph 267), and upon an attack data sent to the target is routed to the guards via a tunnel and then from the guards to the target (paragraphs 252 and 267).

Genty et al and Afek et al are analogous are because they are both related to network protection.

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use the guards and redirection taught in Afek et al with the system in Genty et al because enhanced protection from distributed denial of service attacks is provided (Afek, paragraph 8).

Genty et al in view of Afek et al teaches the limitations as recited above. It fails to teach of reserving for the packet tunnel an amount of bandwidth within an access link, canceling the reserved bandwidth for the packet tunnel and reserving bandwidth for the new packet tunnel. Maeshima et al teaches reserving bandwidth for every IP tunnel on the network (column 3, lines 1-23, 28-32) and reserves the bandwidth once needed (column 5, lines 28-41).

Genty et al in view of Afek et al and Maeshima et al are analogous art because they are related to virtual private network setup.

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use the bandwidth reservation in Maeshima et al with the system in Genty et al in view of Afek et al because it is possible to construct a VPN which enables assurance of bandwidth (Maeshima, column 3, lines 42-46).

Claim 3 discloses the method of claim 1, wherein the source network address and the destination network address comprise Internet Protocol (IP) addresses. Genty et al further teaches the addresses are IP addresses (column 5, lines 1-5).

Claim 4 discloses the method of claim 1, wherein detecting a network attack comprises detecting an attack on the access link coupling a destination network device to a network. Genty et al further teaches an attack can be detected on the network (column 5, lines 48-52).

Claim 6 discloses the method of claim 1, further comprising exchanging a set of available network addresses between a source network device originating the packet tunnel and a destination network device terminating the packet tunnel, wherein the set

of available network addresses correspond to a plurality of intermediate network devices. Genty et al further teaches each device has a set of several addresses, which are exchanged to each device (column 5, lines 34-41).

Claim 7 discloses the method of claim 1, wherein splitting the packet tunnel by selecting an intermediate device comprises: maintaining a set of available network addresses for a plurality of available intermediate network devices, wherein the network addresses are within network address spaces other than the address space of the first local area network and the address space of the second local area network; and selecting one of the network addresses. Genty et al further teaches maintaining a set of available addresses and selecting an address as a net address and making a new tunnel (column 5, lines 34-41, 48-59, 63-67 – column 6, lines 1-6). Afek et al further teaches having multiple sub networks involved which the devices in each sub network would have addresses from their native network address spaces (paragraph 245).

Claim 9 discloses the method of claim 8, further comprising: upon detecting a network attack, sending a message from the destination network device to the source network device instructing the source network device to establish the first packet tunnel with the intermediate network device. Maeshima et al further teaches establishing a first tunnel with an intermediate device (figure 9A, column 4, lines 44-49).

Claim 10 discloses the method of claim 9, further comprising: establishing a secure signaling channel between the source network device and the destination network device; and sending the message via the secure signaling channel. Genty et al

further teaches a virtual private network as a secure connection and sending data over a secure channel (column 1, lines 19-25, figure 7).

Claim 11 discloses the method of claim 1, further comprising de-encapsulating at the intermediate network device packets received from the first packet tunnel; and re-encapsulating the packets at the intermediate network device for communication via the second packet tunnel. Genty et al further teaches encapsulating a packet for transmission through a tunnel and using this encapsulation is widely known in the art (column 4, lines 9-15).

Claim 14 discloses the method of claim 1, wherein reserving an amount of bandwidth comprises sending a reservation message from a destination network device terminating the packet tunnel to a service provider access device. Maeshima further teaches sending a message from a host (column 3, lines 28-32).

Claim 15 discloses the method of claim 14, wherein sending a reservation message comprises sending the reservation message according to the Resource Reservation Protocol (RSVP). Maeshima further teaches using RSVP to reserve the bandwidth (column 3, lines 14-16).

Claim 27 discloses a method comprising: establishing virtual private network service including a packet tunnel having a source network address within an address space of the first local area network and a destination network address within an address space of the second local area network; reserving for the packet tunnel an amount of bandwidth within an access link; detecting a network attack; establishing new virtual private network service upon detecting the network attack, by selecting an

intermediate network device having a network address from a network address space other than the address space of the first local area network and the address space of the second local area network; establishing a first packet tunnel from the first local area network to the intermediate network device; and establishing a second packet tunnel that originates from the intermediate network device to the second local area network; canceling the reserved bandwidth for the packet tunnel after establishing the new virtual private network service; and reserving for the second packet tunnel an amount of bandwidth within the access link upon canceling the reserved bandwidth for the packet tunnel. Genty et al teaches a tunnel between a source and destination (figure 7), an attack is detected (column 5, lines 48-52), a secondary tunnel is established (figure 7), and upon detecting a network attack canceling the bandwidth in the packet tunnel (column 6, lines 31-33). It fails to teach of reserving for the packet tunnels an amount of bandwidth within an access link, in response to the detected network attack, establishing a new virtual private network service by selecting an intermediate network device, wherein the intermediate network device has a network address from a network address space other than the address space of the first local area network and the address space of the second local area network, establishing a first packet tunnel from the first local area network to the intermediate network device, establishing a second packet tunnel that originates from the intermediate network device to the second local area network, and canceling the reserved bandwidth for the packet tunnel. Afek et al teaches a different networks are connected together (paragraph 245), data is diverted to the guards upon detection of an attack which can be from another LAN (paragraphs

250, 252, and 253), data is directed from the source to the guard (paragraph 267), data is sent from the guard to the target (paragraph 267), and upon an attack data sent to the target is routed to the guards via a tunnel and then from the guards to the target (paragraphs 252 and 267).

Genty et al and Afek et al are analogous are because they are both related to network protection.

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use the guards and redirection taught in Afek et al with the system in Genty et al because enhanced protection from distributed denial of service attacks is provided (Afek, paragraph 8).

Genty et al in view of Afek et al teaches the limitations as recited above. It fails to teach of reserving for the packet tunnel an amount of bandwidth within an access link, canceling the reserved bandwidth for the packet tunnel and reserving bandwidth for the new packet tunnel. Maeshima et al teaches reserving bandwidth for every IP tunnel on the network (column 3, lines 1-23, 28-32) and reserves the bandwidth once needed (column 5, lines 28-41).

Genty et al in view of Afek et al and Maeshima et al are analogous art because they are related to virtual private network setup.

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use the bandwidth reservation in Maeshima et al with the system in Genty et al in view of Afek et al because it is possible to construct a VPN which enables assurance of bandwidth (Maeshima, column 3, lines 42-46).

Claim 30 discloses the method of claim 27, wherein detecting a network attack comprises detecting an attack on an access link coupling a destination network device to a network. Genty et al further teaches an attack can be detected on the network (column 5, lines 48-52).

Claim 35 discloses a system comprising a source device coupled to a first local area network; and a destination device coupled to a second local area network, wherein the source device and the destination device establish a packet tunnel having a source network address within an address space of the first local area network and a destination network address within an address space of the second local area network, reserve for the packet tunnel an amount of bandwidth within an access link, upon detecting a network attack, select a new network address from a network address space other than the address space of the first local area network and the address space of the second locale area network, and split the packet tunnel b establishing a first packet tunnel from the first local area network to an intermediate network device having the network address and establishing a second packet tunnel from the intermediate network device to the second local area, wherein the destination device cancels the reserved bandwidth for the packet tunnel after the second packet tunnel is established, and reserves for the second packet tunnel an amount of bandwidth within the access link upon canceling the reserved bandwidth for the packet tunnel and wherein the source device communicates virtual private network (VPN) traffic from the first local area network to the second local area network by redirecting the VPN traffic from the first local area network to the intermediate network device through the first

packet tunnel for forwarding the intermediate network device to the second local area network through the second packet tunnel. Genty et al teaches a tunnel between a source and destination, an attack is detected, a secondary tunnel is established (column 5, lines 48-52, figure 7), and upon detecting a network attack canceling the bandwidth in the packet tunnel (column 6, lines 31-33). It fails to teach of reserving for the packet tunnels an amount of bandwidth within an access link, in response to the detected network attack, splitting the packet tunnel by selecting an intermediate network device, wherein the intermediate network device has a network address from a network address space other than the address space of the first local area network and the address space of the second local area network, establishing a first packet tunnel from the first local area network to the intermediate network device, establishing a second packet tunnel that originates from the intermediate network device to the second local area network, canceling the reserved bandwidth for the packet tunnel and communicating a virtual private network (VPN) traffic from the first local area network to the second local area network by redirecting the VPN traffic from the first local area network to the intermediate network device through the first packet tunnel and forwarding the VPN traffic from the intermediate network device to the second local area network through the second packet tunnel. Afek et al teaches a different networks are connected together (paragraph 245), data is diverted to the guards upon detection of an attack which can be from another LAN (paragraphs 250, 252, and 253), data is directed from the source to the guard (paragraph 267), data is sent from the guard to the target

(paragraph 267), and upon an attack data sent to the target is routed to the guards via a tunnel and then from the guards to the target (paragraphs 252 and 267).

Genty et al and Afek et al are analogous are because they are both related to network protection.

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use the guards and redirection taught in Afek et al with the system in Genty et al because enhanced protection from distributed denial of service attacks is provided (Afek, paragraph 8).

Genty et al in view of Afek et al teaches the limitations as recited above. It fails to teach of reserving for the packet tunnel an amount of bandwidth within an access link, canceling the reserved bandwidth for the packet tunnel and reserving bandwidth for the new packet tunnel. Maeshima et al teaches reserving bandwidth for every IP tunnel on the network (column 3, lines 1-23, 28-32) and reserves the bandwidth once needed (column 5, lines 28-41).

Genty et al in view of Afek et al and Maeshima et al are analogous art because they are related to virtual private network setup.

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use the bandwidth reservation in Maeshima et al with the system in Genty et al in view of Afek et al because it is possible to construct a VPN which enables assurance of bandwidth (Maeshima, column 3, lines 42-46).

Claim 37 discloses the system of claim 35, wherein the source network address and the destination network address comprise Internet Protocol (IP) addresses. Genty et al further teaches the addresses are IP addresses (column 5, lines 1-5).

Claim 38 discloses the system of claim 35, wherein the destination device and the source device comprise edge routers that couple local area networks to the network. Genty et al further teaches the system can be accomplished by routers (column 3, lines 21-26).

Claim 39 discloses the system of claim 35, wherein the destination device detects an attack on an access link coupling the destination device to the network. Genty et al further teaches an attack can be detected on the network (column 5, lines 48-52).

Claim 41 discloses the system of claim 35, wherein the destination device and the source device exchange a set of available network addresses for the source network address and the destination network address of the packet tunnel. Genty et al further teaches each device has a set of several addresses, which are exchanged to each device (column 5, lines 34-41).

Claim 42 discloses the system of claim 35, wherein the destination device comprises a storage medium to store a set of available network addresses for use as the source network address and the destination network address of the packet tunnel. Genty et al further teaches each device has a set of several addresses (column 5, lines 34-41).

Claim 44 discloses the system of claim 35, wherein the intermediate network device de-encapsulates packets received from the first packet tunnel and re-encapsulates the packets for communication to the destination device via the second packet tunnel. Genty et al further teaches encapsulating a packet for transmission through a tunnel and using this encapsulation is widely known in the art (column 4, lines 9-15).

Claim 53 discloses a computer-readable medium comprising instructions to cause a processor to: establish a packet tunnel having a source network address within an address space of a first local area network and a destination network address within an address space of a second local area network; reserve for the packet tunnel an amount of bandwidth within an access link; detect a network attack; in response to the detected network attack, split the packet tunnel by selecting an intermediate network device, wherein the intermediate network device has a network address from a network address space other than the address space of the first local area network and the address space of the second local area network; communicate the network address to the source device for establishing a first packet tunnel from the first local area network to the intermediate network device; establish a second packet tunnel that originates from the intermediate network device to the second local area network; cancel the reserved bandwidth for the packet tunnel; reserve for the second packet tunnel an amount of bandwidth within the access link; and receive virtual private network (VPN) traffic that was redirected from the first local area network to the intermediate network device through the first packet tunnel and forwarded the VPN traffic from the

intermediate network device to the second local area network through the second packet tunnel. Genty et al teaches a tunnel between a source and destination (figure 7), an attack is detected (column 5, lines 48-52), a secondary tunnel can be established with different addresses (column 5, lines 63-67 – column 6, lines 1-6, 20-24), a secondary tunnel is established (figure 7), and upon detecting a network attack canceling the bandwidth in the packet tunnel (column 6, lines 31-33). It fails to teach of reserving for the packet tunnels an amount of bandwidth within an access link, in response to the detected network attack, splitting the packet tunnel by selecting an intermediate network device, wherein the intermediate network device has a network address from a network address space other than the address space of the first local area network and the address space of the second local area network, establishing a first packet tunnel from the first local area network to the intermediate network device, establishing a second packet tunnel that originates from the intermediate network device to the second local area network, canceling the reserved bandwidth for the packet tunnel and communicating a virtual private network (VPN) traffic from the first local area network to the second local area network by redirecting the VPN traffic from the first local area network to the intermediate network device through the first packet tunnel and forwarding the VPN traffic from the intermediate network device to the second local area network through the second packet tunnel. Afek et al teaches a different networks are connected together (paragraph 245), data is diverted to the guards upon detection of an attack which can be from another LAN (paragraphs 250, 252, and 253), data is directed from the source to the guard (paragraph 267), data is

sent from the guard to the target (paragraph 267), and upon an attack data sent to the target is routed to the guards via a tunnel and then from the guards to the target (paragraphs 252 and 267).

Genty et al and Afek et al are analogous are because they are both related to network protection.

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use the guards and redirection taught in Afek et al with the system in Genty et al because enhanced protection from distributed denial of service attacks is provided (Afek, paragraph 8).

Genty et al in view of Afek et al teaches the limitations as recited above. It fails to teach of reserving for the packet tunnel an amount of bandwidth within an access link, canceling the reserved bandwidth for the packet tunnel and reserving bandwidth for the new packet tunnel. Maeshima et al teaches reserving bandwidth for every IP tunnel on the network (column 3, lines 1-23, 28-32) and reserves the bandwidth once needed (column 5, lines 28-41).

Genty et al in view of Afek et al and Maeshima et al are analogous art because they are related to virtual private network setup.

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use the bandwidth reservation in Maeshima et al with the system in Genty et al in view of Afek et al because it is possible to construct a VPN which enables assurance of bandwidth (Maeshima, column 3, lines 42-46).

Claim 55 discloses the computer-readable medium of claim 53, further comprising instructions to cause the processor to select the intermediate network device by: maintaining a set of available network addresses; and selecting one of the network addresses. Genty et al further teaches maintaining a set of available addresses and selecting an address as a net address and making a new tunnel (column 5, lines 34-41, 48-59, 63-67 – column 6, lines 1-6).

Claims 2 and 36 are rejected under 35 U.S.C. 103(a) as being unpatentable over Genty et al (US Patent #6,473,863) in view of Afek et al (US PGPUB US2002/0083175) in view of Maeshima et al (US Patent #6,092,113) as applied to claims 1 and 35 above, and further in view of Adams et al (US PGPUB US2003/0016679).

Claims 2 and 36 disclose the method and system of claims 1 and 35 wherein the source network address and the destination network address comprise port numbers. Genty et al in view of Afek et al in view of Maeshima et al teaches the limitations of claims 1 and 35 as recited above. It fails to teach of the addresses comprising of port numbers. Adams et al teaches control information being an IP address or a port number among other information (paragraph 21, lines 1-8).

Genty et al in view of Afek et al in view of Maeshima et al and Adams et al are analogous art because they are both related to routing data over a network.

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use the control information in Adams et al with the system in Genty et al in view of Afek et al in view of Maeshima et al because the packet is able to be sent to its next destination once the information is known (Adams, paragraph 21, lines 8-12).

Claims 12, 13, 45, and 46 are rejected under 35 U.S.C. 103(a) as being unpatentable over Genty et al (US Patent #6,473,863) in view of Afek et al (US PGPUB US2002/0083175) in view of Maeshima et al (US Patent #6,092,113) as applied to claims 8 and 43 above, and further in view of Jorgensen (US PGPUB US2002/0099854).

Claim 12 discloses the method of claim 1, further comprising: establishing a secure signaling channel between a source network device and a destination network device; sending via the secure signaling channel control packets between the source network device and the destination network device to monitor the performance of the first and second packet tunnels; and selecting a new intermediate network device when the performance reaches a minimum threshold. Genty et al in view of Afek et al in view of Maeshima et al teaches the limitations of claim 8 as recited above. It fails to teach of sending messages to monitor performance and making changes based on performance. Jorgensen teaches monitoring, control, service, modify and repair a system by sending messages monitoring the performance and making changes based on performance (paragraph 612).

Genty et al in view of Afek et al in view of Maeshima et al and Jorgensen are analogous art because they are related to network setup and control.

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use the monitoring in Jorgensen with the system in Genty et al in view of Afek et al in view of Maeshima et al because proactive provisioning of additional resources can occur (Jorgensen, paragraph 612, lines 7-9).

Claim 13 discloses the method of claim 12, further comprising maintaining a set of possible intermediate network devices for a plurality of available intermediate network devices, wherein the network addresses are within network address spaces other than the address space of the first local area network and the address space of the second local area network, and wherein selecting the intermediate network device comprises selecting one of the possible intermediate network devices from the set. Genty et al further teaches each device has a set of several addresses, which are exchanged to each device, and the second device is selected from this list (column 5, lines 34-41).

Claim 45 discloses the system of claim 35, wherein the source device and the destination device establish a secure signaling channel and send via the secure signaling channel control packets to monitor the performance of the first and second packet tunnels. Genty et al in view of Afek et al in view of Maeshima et al teaches the limitations of claim 43 as recited above. It fails to teach of monitoring performance. Jorgensen teaches monitoring, control, service, modify and repair a system by sending messages monitoring the performance (paragraph 612).

Genty et al in view of Afek et al in view of Maeshima et al and Jorgensen are analogous art because they are related to network setup and control.

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use the monitoring in Jorgensen with the system in Genty et al in view of Afek et al in view of Maeshima et al because proactive provisioning of additional resources can occur (Jorgensen, paragraph 612, lines 7-9).

Claim 46 discloses the system of claim 45, wherein the destination device selects a new intermediate network device when the performance reaches a minimum threshold. Jorgensen further teaches making changes based on the performance when monitoring (paragraph 612).

Claims 16, 17, and 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Genty et al (US Patent #6,473,863) in view of Afek et al (US PGPUB US2002/0083175) in view of Maeshima et al (US Patent #6,092,113) as applied to claims 1 and 27 above, and further in view of Shawcross (US Patent #6,880,090).

Claim 16 discloses the method of claim 1, wherein establishing a packet tunnel comprises: maintaining a set of available multicast network addresses; selecting one of the multicast network addresses for the packet tunnel; and subscribing to a multicast channel for the selected multicast network address. Genty et al in view of Afek et al in view of Maeshima et al teaches the limitations of claim 1 as recited above. It fails to teach of using multicast addresses. Shawcross teaches maintaining a set of multicast addresses, selecting a multicast address and subscribing to the multicast addresses (column 5, lines 60-67, column 6, lines 1-5).

Genty et al in view of Afek et al in view of Maeshima et al and Shawcross are analogous art because they are related to network attack prevention.

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use the multicast addressing in Shawcross with the system in Genty et al in view of Afek et al in view of Maeshima et al because the technique prevents

unauthorized personnel from knowing which address to disrupt (Shawcross, column 6, lines 12-14).

Claim 17 discloses the method of claim 16, wherein establishing a second packet tunnel comprises: unsubscribing to the multicast channel; selecting one of the multicast network addresses for the destination network address; establishing the second packet tunnel using the new destination address; and subscribing to a multicast channel for the selected multicast network address. Shawcross further teaches unsubscribing the multicast channel, selecting a multicast channel, establishing a new tunnel and subscribing to a multicast addresses (column 2, lines 62-67 – column 3, lines 1-17, column 9, lines 5-10, 36-42).

Claim 29 discloses the method of claim 27, wherein establishing a packet tunnel comprises: maintaining a set of available multicast network addresses; selecting one of the multicast network addresses for the destination network address of the packet tunnel; and subscribing to a multicast channel for the selected multicast network address. Genty et al in view of Afek et al in view of Maeshima et al teaches the limitations of claim 27 as recited above. It fails to teach of using multicast addresses. Shawcross teaches maintaining a set of multicast addresses, selecting a multicast address and subscribing to the multicast addresses (column 5, lines 60-67, column 6, lines 1-5).

Genty et al in view of Afek et al in view of Maeshima et al and Shawcross are analogous art because they are related to network attack prevention.

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use the multicast addressing in Shawcross with the system in Genty et al in view of Afek et al in view of Maeshima et al because the technique prevents unauthorized personnel from knowing which address to disrupt (Shawcross, column 6, lines 12-14).

***Response to Arguments***

Applicant's arguments filed April 30, 2007 have been fully considered but they are not persuasive.

Applicant asserts the prior art fails to teach selecting the guard devices in response to the detected network attack. The Examiner respectfully disagrees, Afek et al teaches the guards are notified and then used therefore being selected to have the traffic directed through the guards (paragraphs 252 and 257).

Applicant asserts the prior art fails to teach the guard device having a network address from a network address space other than the address space of the first local area network and the address space of the second local area network. The Examiner respectfully disagrees, Afek et al teaches the devices may be separated from each other in separate networks therefore having addresses in different address spaces (paragraphs 243 and 245).

Applicant asserts the prior art fails to teach establishing a first packet tunnel from the first local area network to the intermediate network device and establishing a second packet tunnel that originates from the intermediate network device to the second local area network. The Examiner respectfully disagrees, Afek et al teaches the traffic

is directed from the source to the guard and then the traffic is sent from the guard to the device, these paths are interpreted as tunnels (paragraph 267).

***Conclusion***

**THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Brian J. Gillis whose telephone number is 571-272-7952. The examiner can normally be reached on M-F 7:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Rupal Dharia can be reached on 571-272-3880. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Brian J Gillis
Examiner
Art Unit 2141

BJG
6/7/2007

RUPAL DHARIA
SUPERVISORY PATENT EXAMINER